iSecurity

DATASHEET

Field Encryption

Need for Encryption

Data encryption is an increasingly essential element of effective computer security systems. It is the final layer of protection for your business-critical data from those who managed to pass through other protection techniques that you may have. So, even if the data is accessed, it is entirely meaningless.

Encryption is also the way to ensure that sensitive data is presented in the way that suits the user, and the circumstances. Those who are entitled to access your data will see the data in clear text, masked, scrambled, or not see it at all, as appropriate.

PCI-DSS, HIPAA, GDPR and other regulatory bodies require encrypting sensitive parts of the data.

Raz-Lee Security’s iSecurity Field Encryption solution, part of the iSecurity suite, allows you to fully protect all sensitive data without modifying your software. A change that is done externally without changing the Level-Check of your file (i.e. Files remain intact), but is reflected in:

- Your programs, regardless of whether they use SQL or Native IO
- Any system utility including FTP, Query, DFU
- DB-Journal

IBM i 7.1 introduced the database exit program FIELDPROC. Using this feature for encryption makes it part of the database capabilities and eliminates use of additional files. iSecurity Encryption was designed after the FIELDPROC announcement and does not need to have backward capability with outdated technology – providing efficiency and simplicity.

Data remains encrypted in all circumstances

A known disadvantage of the wonderful FIELDPROC capability is that if the commonly used command Change Physical File (CHGPF) with the SRCFILE parameter is used against an encrypted file, the file becomes decrypted without any warning. iSecurity Encryption has been designed with a checks and balances system to prevent CHGPF with SRCFILE option from causing all Field Procedures to decrypt all the encrypted data in the file. Before being processed, the user (if in an interactive session) or the QSYSOPR must confirm the action. Even when confirmed, an alert is sent as a further measure of security. If the user is not allowed to see the decrypted data, iSecurity Field Encryption stops the process of CHGPF.

In addition, an independent "Watch-Dog" system ensures that encryption of fields is in place. It is possible to define which encrypted fields alerts should be sent about. A special option allows to set it so that it will be alerted only after the first encryption.

Finding Sensitive Data Fields

A fully comprehensive system is provided to help you discover ALL your sensitive fields. All database fields are considered and the product offers selection aids based on field size, name, text, and column headings. This prevents a situation where sensitive data is kept in the clear in a forgotten, copied version of a file.

Product Features

Unique design provides a more efficient product, which ensures that making your data safer does not require you to invest in additional resources.

With iSecurity Encryption:

- Files are never locked; they are available for application use even when encryption keys are refreshed.
- Supports all types of data: Character, Zoned Decimal, Packed Decimal, Clob and Blob. Supports null-capable data as well as non-null-capable data.
- Comprehensive Find Sensitive Fields system provides superior quality in finding based on iterations over partial estimation of size, type, name, text…
- Get trillions of encryption combinations that each can be decrypted to its original value.

- Saves time – Copy the definitions Defining who can see decrypted fields: This is based on the current user of the job, BUT exceptions can be given based on the program that is used, the record format of the display file and through an API.
- Works on a wrapper program thus does not require the program source.
- Optimized for data masking and consumes no CPU for decryption in such cases.
- KEK (Key encrypting Keys) as well as Data Keys can be automatically changed, unattended.
- In a multi-site environment, a single key manager can be set to support all sites, centralizing all keys-related activity.
- Optimized to display the standard masked data. Choosing this option greatly reduces performance impact.
- Key Manager, Data Manager, and Token Manager can optionally be installed on different IBM i LPARs.
- Supports both Encryption and Tokenization.
- Maintains unencrypted sort settings that have been activated prior to encryption.
- Policy driven security and limitation of capabilities ensures Separation of Duties.
- Comprehensive logs for tracing of activities.
- Full journaling system guarantees that any change in parameters is logged.
- Uses NIST encryption standards.
- Adheres to both GDPR, PCI and COBIT standards.
- 128-bit, 192-bit, and 256-bit AES encryption supported.
- Based on IBM Native APIs.